Pangea for Securing AI Software

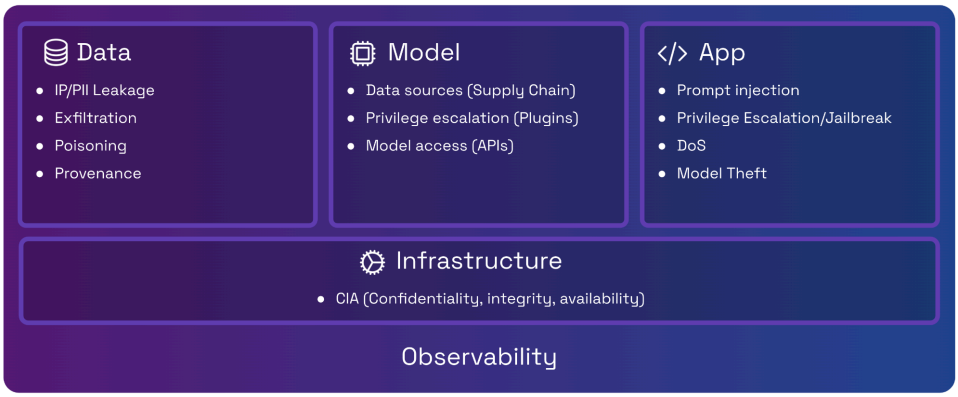
Solution Brief

Accelerate Delivery of Secure, AI-Powered Apps with Composable Security

THE AI INSIDE THREAT

As product teams seek to embed AI and LLM technologies in their applications, security teams are overwhelmed by a barrage of new compliance and security risks around sensitive data leakage and the threat of AI itself becoming an attack vector. These risks arise because AI applications must train on or gain persistent access to corporate data to deliver personalized interactions to customers and employees. Developers fuse enterprise data with AI via architectures like agents, RAG, fine tuning, and micro LLMs, but all fusion methods raise serious security concerns, such as:

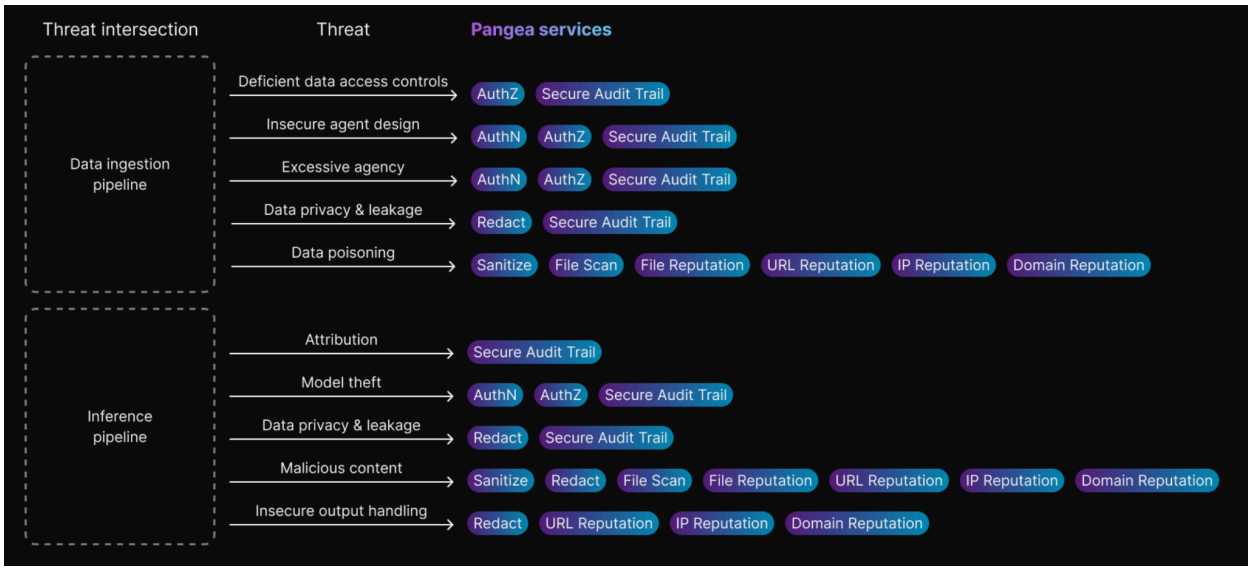
- **Data access control**: does the user who made the prompt request have authorization to view the context being fetched from an internal database to enrich the response?
- **Excessive agency**: can the AI agent execute commands or APIs that could cause harm to the organization such as the deletion of critical file systems or enable lateral movement?
- **Malicious content**: do the prompt inputs, LLM responses, or contextual data from an external source contain malicious URLs, domains or files that could infect internal systems or end users?



Relying on developers to self-engineer security guardrails to address these AI threats can introduce unintended vulnerabilities and misconfigurations, and gives security teams limited if any visibility and configuration control to manage the risk posture of AI-powered software.

PANGEA COMPOSABLE SECURITY FOR AI

Pangea's Composable Security Platform gives developers a paved path to build AI-powered software quickly and securely with 19 pre-built, API-driven security features such as AI prompt logging, sensitive data redaction, and agent-specific authorization. Deployed with just a few lines of code, Pangea mitigates security threats across both the AI data ingestion and inference pipelines when building software products:



Pangea also provides a SaaS configuration control plane so that security and risk teams can see and adjust feature-level risk postures of AI-powered apps in real-time, without requiring any code changes.

Deploy Flexibly

Deploy AI security wherever you need it: Pangea is app, cloud, framework & LLM agnostic.

Launch Quickly

Take AI-powered apps to market quickly and confidently with approved security guardrails.

Reduce Security Risk

Secure data, apps, models, and end users from sensitive data leakage, theft, malware, and more.

To find out how Pangea can help secure your AI-powered software and mitigate risks in AI architectures like agents, RAG, fine tuning, and micro LLMs, please contact us at: https://pangea.cloud/contact-us/.